computing@computingonline.net
www.computingonline.net

Print ISSN 1727-6209
On-line ISSN 2312-5381
International Journal of Computing

COMBINING AND FILTERING FUNCTIONS IN THE FRAMEWORK OF NONLINEAR-FEEDBACK SHIFT REGISTER

Alexandr Kuznetsov [1,2], Oleksandr Potii [1,2], Nikolay Poluyanenko [1,2], Oleksii Smirnov [3], Igor Stelnyk [4], Danylo Mialkovsky [4]

[1] V. N. Karazin Kharkiv National University, Svobody sq., 6, Kharkiv, 61022, Ukraine
[2] JSC "Institute of Information Technologies", Bakulin St., 12, Kharkiv, 61166, Ukraine,
kuznetsov@karazin.ua, potav@ua.fm, nlfsr01@gmail.com
[3] Central Ukrainian National Technical University, University Avenue 8, Kropyvnytskyi, 25006, Ukraine,
dr.SmirnovOA@gmail.com
[4] Department of Information Protection Administration of the State Service of Special Communication and Information Protection of Ukraine, Solomianska 13 str., Kyiv, 03680, Ukraine,
stelnik_i@i.ua, mdv@dsszzi.gov.ua

Paper history:
Received 14 January 2019
Received in revised form 14 February 2020
Accepted 17 February 2020
Available online 14 June 2020

Keywords:
stream ciphers;
generators of the pseudorandom sequence;
NLFSR;
nonlinear feedback shift register;
filtering function;
combining function;
cryptanalysis;
nonlinear polynomials.

Abstract: Strong cryptography of stream ciphers is determined according to the ability of the generated pseudorandom sequence to resist analytical attacks. One of the main components of the pseudorandom stream cipher sequence generating algorithm is Boolean functions for combining and filtering. The paper considers the possibility of applying nonlinear-feedback shift registers that generate a maximum length sequence as a combining or filtering function. The main indicators of cryptographic strength of such functions as: balance, the prohibitions presence, correlation immunity and nonlinearity are examined in this work. The study analyzes and demonstrates correlation immunity and nonlinearity experimental values for all nonlinear feedback shift registers that generate a maximum length sequence, for register sizes up to 6 cells inclusively, and register sizes up to 9 cells inclusively with algebraic degree of the polynomial under 2. The possibility of optimizing the process of selecting Boolean functions according to the criteria of maximum correlation immunity and nonlinearity with various algebraic degrees and minimization of the number of monomials in the polynomial is studied.

1. INTRODUCTION

1.1 RESEARCH MODEL

In the general block diagram of a combination generator (Fig. 1) and filter generator (Fig. 2) of the pseudorandom sequence (PRS) that use several linear-feedback shift registers (LFSR) or nonlinear-feedback shift registers (NLFSR), – $SR_i\ (i=1,\dots,L)$, the function f is usually considered either a combination or a filtering function of L variables.

In general, a Boolean reflection $f: GF_2^L \to GF_2$ is a Boolean function that corresponds to NLFSR. Boolean functions will be represented in the form of polynomials (a Zhegalkin polynomial or an algebraic normal form - ANF) in a field F_2:

$$f(x_1,\dots x_L) = \bigoplus_{N\in P\{1,2,\dots,L\}} a_N \prod_{i\in N} x_i\ , \qquad (1)$$

where $P\{1,2,\dots,L\}$ is the set of all subsets $\{1,2,\dots,L\}$ (Boolean), $a_N \in F_2$.

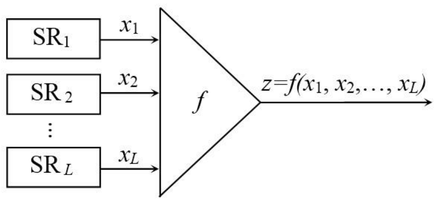

Figure 1 – Block diagram of a combination PRS generator

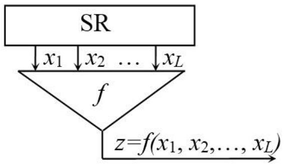

Figure 2 – Block diagram of a filter PRS generator

The paper will investigate only those NLFSRs that form a modified de Bruijn sequence (which is the maximum length sequence, i.e., M-sequence). Such nonlinear registers are denoted as M-NLFSR.

1.2 THE STUDIED CRYPTOGRAPHIC PROPERTIES OF M-NLFSR

In this particular case, some of the main indicators of cryptographic stability evaluation examined are:

- Balance.

Boolean function f of L variables is called balanced if the function takes values 0 and 1 with equal frequency. This is one of the most natural properties of the Boolean functions that are used in stream ciphers [1].

If the Boolean function is balanced, then the probability will take a value of 0 or 1 that is the same and equals 1/2. This allows us to reduce the statistical dependencies between the function input and output. In other cases, the analyst has the possibility to cryptanalyze the cipher using the distribution of all relations.

- Prohibition presence

The PRS analysis that is generated by the filtering generator causes a Boolean function prohibition, i.e., the presence of the initial sequence combinations, which is prohibited in every combination of the input sequence.

It is intuitively clear that the presence of a prohibition in the filtering function of the generator makes it "weaker", this prohibition will never appear in the initial sequence of the generator, which impairs its statistical properties.

- Correlation immunity.

The correlative immune function requirement is related to the correlation attack counteraction, the idea of which is as in [2]. In a combination PRS generator (Fig. 1) the key to the generator is the initial state of all registers. The key volume equals to $2^{l_1+\ldots+l_L}$, where l_i is the length of SR_i for $i=1,\ldots,L$.

Each of the SR_i generates $x_i = x_i^1 x_i^2 \ldots$ sequence that is usually close to the random one in regard to its properties. In particular, with a fairly large sequence length for its randomly selected bit x_i^j (where j in x_i^j is the number of the bit in the sequence x_i), there is a probability of a random event $x_i^j=0$: $\mathrm{P}[x_i^j=0]\approx 1/2$. Thus, if $y=y^1y^2\ldots$ is a random sequence that does not depend on x_i, then

$$\begin{aligned}&\mathrm{P}[x_i^j=y^j]=\mathrm{P}[x_i^j=0]\cdot\mathrm{P}[y^j=0]+\\&+\mathrm{P}[x_i^j=1]\cdot\mathrm{P}[y^j=1]\approx\\&\approx 1/2\cdot\left(\mathrm{P}[y^j=0]+\mathrm{P}[y^j=1]\right)=1/2\end{aligned}\quad . \qquad (2)$$

Let us assume, that $\mathrm{P}[f=x_1]\neq 1/2$ (in this case it is said that the function f correlates with the variable x_1). Using a correlation attack, the initial state of s_1 SR_1 can be found. To do so, one should go over all the possible 2^{l_1} of the SR_1 states, for each of them a sequence $z'=z'_1z'_2\ldots$ is created and the number of matches with PRS $z'_i=z_i$ is counted. For all sequences, except for one (generated by s_1), a part of matches will be $\approx 1/2$. By that we define that the part of the key is the s_1 state. If the function f has a correlation with all its variables (or with all but one - then the state of the register corresponding to this variable, will be found the last, with the information about all other registers' state), then the generator key is found in $2^{l_1}+\ldots+2^{l_L}$ tries, which is much less complicated.

- Nonlinearity.

In practice [3-5] the cryptographic transformations, which have properties close to those of linear functions, in many cases lead to a significant decrease in the cipher stability. That is why, the functions, whose properties exclude the weaknesses typical of the functions close to the linear ones, play an important role in cryptography. Thus, the desired property of a function is its nonlinearity that is given a broad meaning: as an opposition to linearity. In block and stream ciphers, the application of a high nonlinearity function increases the cipher stability in regard to the linear and differential cryptanalysis methods.

1.3 PROBLEM STATEMENT

A lack of description of different cryptographic properties connection is observed in literature. In work [1], as cipher components, it is necessary to choose the functions that are "good from every side", which in reality is a very difficult task, since many properties contradict each other. Although the theoretical results show that in a random function, many cryptographic parameters are close to optimal ones. The question is how to choose it?

In addition to optimizing cryptographic performance, in practical implementation it is necessary to take into account the simplicity of implementation (both software and hardware). The less resources (memory, the number of simple operations - in software implementation; the logical elements and the possibility of their parallelization - in hardware) are spent by the algorithm to form the next bit, the higher is the possibility to get a faster, cheaper in manufacturing, and less energy-consuming final product.

The work can be viewed as an extension of the materials obtained by the authors and stated in [3-5] for the case of using ANF with nonlinearity of a random order. The results presented in [3-5] are given here for integrity.

The article analyzes the possibility of using M-NLFSR as either a combination or filtering function. It also studies the problem of M-NLFSR selection optimization by the criteria of maximum correlation immunity and nonlinearity at different algebraic degrees, as well as the possibility of minimizing the number of monomials used.

1.4 DEFINITIONS USED

F_2 – the final field of two elements, 0 and 1.

V_L – L-dimensional vector space over the F_2 field, $V_L = (F_2)^L$. Addition in space V_L bitwise exclusive disjunction.

$A = a_1, a_2, \ldots, a_{2^L-1}, a_{2^L}$ is a sequence with the length 2^L from the elements of the alphabet $\{0,1\}$.

A is a de Bruijn sequence of order L if among all the tuples with the length L: $(a_1, a_2, \ldots, a_L)$, $(a_2, a_3, \ldots, a_{L+1})$, …, each of the possible tuples is present and occurs exactly once, i.e., all possible 2^L combinations of the alphabet $\{0,1\}$ are present [6].

Similar sequences ($2^L - 1$) without tuples from only zeros are called the *modified de Bruijn sequences.*

The degree of a monomial (a Boolean monomial) $x^N = \prod_{i \in N} x_i$ is defined as $|N|$ (the number of elements of the subset N).

The algebraic degree $\deg(f)$ or *the degree of nonlinearity* of a Boolean function f is the number of variables in the longest addend (monomial) of its ANF. A Boolean function of 1 degree is called affine. Its ANF looks like

$$f(x) = a_1 x_1 \oplus a_2 x_2 \oplus \ldots \oplus a_L x_L \oplus b, \qquad (3)$$

where $b \in F_2, a \in V_L$. If $b = 0$ then the function is called linear, and the corresponding shift register is LFSR. A function is called quadratic, cubic, etc., if its algebraic degree is 2, 3, etc., respectively. The function $\deg(f) = 1$ is an affine function. The case of the affine function is $a_0 = 0$ according to the linear function. The set of affine Boolean functions from L variables is denoted as A_L.

Hamming weight or simply the weight of a binary vector is the number of units among its components. The Hamming weight of a Boolean function is the weight of the vector of its values. The weight of a vector or function is denoted by $wt(x)$ and $wt(f)$.

Hamming distance $dist(f, g)$ between the two functions f and g is the weight of the function $f \oplus g$. In other words, it is the number of those $x \in V_L$ for which $f(x) \neq g(x)$ is true.

Nonlinearity N_f of a Boolean function f is the Hamming distance between f and the set of affine functions.

A “*maximally nonlinear function*” is such Boolean function of L variables (L can equal anything) that the Hamming distance from a given function to the set of all affine functions is maximally possible. In case L is even, the maximum possible value of nonlinearity equals ($2^{L-1} - 2^{(L/2)-1}$). In case L is odd, the exact value of the maximum distance is unknown. The term “maximally nonlinear function” can be seen in Ukrainian literature, whereas in English, the term “bent function” is more typical. The analogy between the terms is not complete. For an even number of variables L, bent functions and maximally nonlinear functions coincide, however for an odd L, bent functions (unlike maximally nonlinear functions) do not exist. In addition, all bent functions are not balanced (unlike the functions of the corresponding M-NLFSR, as it will be shown below), which makes them vulnerable to statistical analysis.

2. RESULTS

2.1 BALANCE

M-NLFSR, as does M-LFSR, generates a modified de Bruijn sequence, and if we add to the consideration the state of filling all cells with nulls, then the resulting function will be balanced. In the equally probable and independent selection of Boolean function f arguments, which forms the M-NLFSR, the probabilities of its values, respectively, are equal

$$P(1) = wt(f)/2^L, \quad P(0) = 1 - wt(f)/2^L.$$

2.2 PROHIBITIONS PRESENCE

M-NLFSR are functions that have no prohibitions. This is due to the fact that the NLFSR forms a de Bruijn sequence that, by definition, has all the possible combinations of sequence.

However, one should be careful, since a fully balanced filtering function in one form or other transfers the properties of the input sequence to the generated sequence [7]. For example, in work [8], was established a new criterion, that states: "the filtering function preserves prohibitions (in the corresponding sense) only if it is completely balanced". Thus, if the input function enters a sequence "far" from a random one, then its statistical properties will be poor in the output.

2.3 CORRELATION IMMUNITY

The statements and theorems given in this and the next sections are aimed at reducing the amount of work, and are given without proof. The latter is public and is shown, for example, in [1-2, 9-11].

The presence of a correlative immune function of the degree m means that the values of the function $Z = f(X)$ are statistically independent of any set from, at most, m components of a random argument vector $X = (F_2)^L$. This is equivalent to the condition that the output of the transformation does not include information about the vectors from the input of the transformation and that has a Hamming weight of no more than m.

Boolean function f is called correlatively immune to the order m, $1 \le m \le L$, if for any set of numbers m of the variables

$$1 \le i_1 < i_2 < \ldots < i_m \le L$$

the random variables $X = \left(x_{i_1}, x_{i_2}, \ldots, x_{i_m}\right)$ and $Y = f\left(x_1, x_2, \ldots, x_L\right)$ are independent.

The fact that the function, which is correlation immune to the order m of the L variables is correlation immune to a random smaller order. Thus, the Boolean function f corresponds to some maximum order of its correlation immunity $m_{\max}$, which is denoted by $cor(f)$.

$m = L$ can only be true, if $f = const$. Only affine functions can reach the maximum correlation immunity of $m = L-1$ degree, i.e., cryptographically weak ones. In addition, if f is balanced and $cor(f) = L-2$, then the function f is also affine. Thus, it makes sense to consider the order of correlation immunity m only in the range of $1 \le m \le L-3$.

The balanced correlation-immune function of the order m is called m*-stable*. Technically, any balanced Boolean function can be considered as a 0-stable and a random Boolean function as (-1)-stable. Similarly to $cor(f)$ a denotation of the maximum stability order is introduced:

$$sut(f) = \begin{cases} -1, & \text{if } f \text{ is not balanced}, \\ cor(f), & \text{if } f \text{ is balanced}. \end{cases}$$

Siegentaler's inequality. If f is a function in $(F_2)^L$ that is correlation immune to order m, then:

1. $deg\left(f\right) \le L - m$;
2. if f is balanced and $sut(f) = m \le L-2$, then $deg(f) + sut(f) \le L-1$.

Siegentaler's inequality is one of many contradictions in the cryptographic properties of functions: the high order of the correlation immune function entails its low algebraic degree and vice versa.

If the function f is balanced, $sut(f) = m \le L-2$ and $\deg(f) = L-m-1$, then f is called m*-optimal*.

Thus, there are m-optimal f for LFSR $m = L-1-\deg(f) = L-2$ and for the second-order NLFSR $m = L-1-\deg(f) = L-3$, etc. The value of the maximum stability order for m-optimal functions, depending on the length of the register and the algebraic degree, is given in Table 1.

Table 1. The value of the maximum stability order for m-optimal functions

	L						
	3	4	5	6	7	8	9
M-LFSR	1	2	3	4	5	6	7
M-NLFSR 2nd order	0	1	2	3	4	5	6
M-NLFSR 3nd order	–	0	1	2	3	4	5
M-NLFSR 4nd order	–	–	0	1	2	3	4

Thus, we have defined the upper limit of values for m-resistant functions. The work investigated the correlation immunity of the entire M-NLFSR set sized $2 \le L \le 6$ (the results are presented in Table 2), as well as the M-LFSR and M-NLFSR 2nd order for $L \le 9$ (see Table 3).

As it can be seen in Tables 2-3, M-NLFSR reach the values for the m-optimal functions (in the table these are designated as “m”) for all studied L. However, there is a very large proportion (approximately half of the entire 2nd order M-NLFSR set if $7 \le L \le 9$ and 2/3 if $L = 6$), which has no correlation immunity.

Table 2. The distribution of the number of registers depending on the maximum stability for M-NLFSR

$sut(f)$	Number of M-LFSR	Number of 2nd order M-NLFSR	Number of 3rd order M-NLFSR	Number of 4th order M-NLFSR
$L=2$				
m=0	0	–	–	–
m=1	1	–	–	–
$L=3$				
m=0	0	–	–	–
m=1	^{m} 2	–	–	–
$L=4$				
m=0	0	4	–	–
m=1	2	^{m} 10	–	–
m=2	0	–	–	–
$L=5$				
m=0	0	64	1024	–
m=1	2	52	^{m} 896	–
m=2	0	^{m} 6	–	–
m=3	^{m} 4	–	–	–
$L=6$				
m=0	0	788	1434988	44586880
m=1	2	1044	640762	^{m} 20424832
m=2	0	76	^{m} 19450	–
m=3	4	^{m} 38	–	–
m=4	0	–	–	–

Table 3. The distribution of the number of registers depending on the maximum sustainability for M-PCNOS if $deg(f) \le 2$.

$sut(f)$	Number of M-NLFSR	Number of M-LFSR	Number of 2nd order M-NLFSR
$L=7$			
m=0	33 988	0	33 988
m=1	25 582	4	25 578
m=2	4 090	0	4 090
m=3	388	10	378
m=4	4	0	^{m} 4
m=5	4	^{m} 4	–
$L=8$			
m=0	1 686 218	0	1 686 218
m=1	2 120 124	0	2 120 124
m=2	194 798	0	194 798
m=3	16 624	12	16 612
m=4	188	0	188
m=5	46	4	^{m} 42
m=6	0	0	–
$L=9$			
m=0	284 956 836	0	284 956 836
m=1	208 843 950	2	208 843 948
m=2	24 325 344	0	24 325 344
m=3	1 091 584	16	1 091 568
m=4	21 192	0	21 192
m=5	876	28	848
m=6	10	0	^{m} 10
m=7	2	^{m} 2	

2.4 NONLINEARITY

Nonlinearity of function f, as it is mentioned above, is the distance from f to the class of affine functions A_L:

$$N_f = dist(f, A_L) = \min_{g \in A_L} dist(f, g). \quad (4)$$

The following statements show that the higher the order of the correlation immune function is, the lower the top limit of its nonlinearity is.

If f is balanced and m-stable, $m \le L-2$. Then

$$N_f \le 2^{L-1} - 2^{m+1}.$$

Similarly, with the notion of the m-optimal function, a special name for the m-stable functions of the maximum possible nonlinearity is introduced.

If the function f with $(F_2)^L$ is balanced,

$$sut(f) = m \le L-2$$

and

$$N_f = 2^{L-1} - 2^{m+1},$$

then f is called m-*saturated*.

Table 4 shows the calculated values of the formulas above with the maximum possible nonlinearity of the balanced function, depending on its stability.

Table 4. Values of non-linearity of m-saturated functions depending on their maximum stability.

	$sut(f)$						
	0	**1**	**2**	**3**	**4**	**5**	**6**
$L=3$	2	0	–	–	–	–	–
$L=4$	6	4	0	–	–	–	–
$L=5$	14	12	8	0	–	–	–
$L=6$	30	28	24	16	0	–	–
$L=7$	62	60	56	48	32	0	–
$L=8$	126	124	120	112	96	64	0
$L=9$	254	252	248	240	224	192	128

However, the value of the nonlinearity given in Table 4 is not necessarily achievable. Let us denote a *maximally possible nonlinearity* of m-stable Boolean function given in $(F_2)^L$ as $N_{f\,max}(L,m)$ and provide the upper estimate for nonlinearity of m–resistant functions.

Considering the above, it is clear that $N_{f\,max}(L,-1) = 2^{L-1} - 2^{L/2-1}$, this value can be achieved only for even L. If f is a balanced function and L is even, it is true, that $N_{f\max}(L,m) = 2^{L-1} - 2^{L/2-1} - 2^{m+1}$ [2].

In [12] it is indicated that for odd L and $L \le 7$, $N_{f\max}(L,-1) = 2^{L-1} - 2^{(L-1)/2}$, but for odd L and $L \ge 15$ $N_{f\max}(L,-1) > 2^{L-1} - 2^{(L-1)/2}$ is true.

When $m \ge L-2$, according to Siegentaler's inequality $\deg(f) \le 1$, thus $N_{f\max}(L,m) = 0$. Also [12] refers to the proved inequality $N_{f\max}(L,L-3) = 2^{L-2}$ and the hypothesis that $N_{f\max}(L,L-4) = 2^{L-1} - 2^{L-3}$. In addition, some exact values of $N_{f\max}(L,m)$ are given for small L and m:

$$N_{f\max}(4,0) = 4;$$
$$N_{f\max}(5,-1) = N_{f\max}(5,0) = N_{f\max}(5,1) = 12;$$
$$N_{f\max}(6,0) = 26; N_{f\max}(6,1) = N_{f\max}(6,2) = 24;$$
$$N_{f\max}(7,-1) = N_{f\max}(7,0) = N_{f\max}(7,1) = 56.$$

These results do not contradict with the results obtained in this work and given below.

The obtained results of the distribution on the non-linearity of the entire set of M-NLFSR sized below $L \le 6$ are summarized in Table 5.

Table 5. The distribution of the number of registers depending on nonlinearity

N_f	Number of M-LFSR	Number of 2nd order M-NLFSR	Number of 3rd order M-NLFSR	Number of 4th order M-NLFSR
$L=2$				
0	1			
$L=3$				
0	2			
$L=4$				
0	2			
4		14		
$L=5$				
0	6			
4			296	
8		66	1624	
12		56		
$L=6$				
0	6			
4				1 424
8			2 892	80 004
12			57 688	1 844 824
16		350	615 116	19 851 036
20			988 840	42 826 836
24		1 596	430 664	407 588

The Tables 6 and 7 summarize the distribution results for $L \le 6$, depending on the nonlinearity and the maximum order of stability, and the Tables 8 and 9 contain similar results for the 2nd order M-NLFSR if $7 \le L \le 9$.

Table 6. The number of registers distribution depending on nonlinearity and maximum stability for M-NLFSR (if $L \le 6$ $\deg(f) = 1,2$)

N_f	Number of M-LFSR				Number of 2nd order M-NLFSR			
	$sut(f)$, if $m=$				$sut(f)$, if $m=$			
	0	1	2	3	0	1	2	3
$L=2$								
0		1	–	–	–	–	–	–
$L=3$								
0		^{m} 2	–	–		–	–	–
$L=4$								
0		2		–			–	–
4			–	–	4$^{1)}$	^{m} 10	–	–
$L=5$								
0		2		^{m} 4				–
4				–				–
8				–	8	52	^{m} 6	–
12			–	–	56$^{1)}$		–	–
$L=6$								
0		2		4				
4								
8								
12								
16					48	188	76	^{m} 38
20				–				–
24				–	740	856$^{1)}$		–

Table 7. The number of registers distribution depending on nonlinearity and maximum stability for M-NLFSR (if $L \le 6$ $\deg(f) = 3,4$)

N_f	Number of 3rd order M-NLFSR			Number of 4th order M-NLFSR	
	$sut(f)$, if $m=$			$sut(f)$, if $m=$	
	0	1	2	0	1
$L=2$					
0	–	–	–	–	–
$L=3$					
0	–	–	–	–	–
$L=5$					
0			–	–	–
4	128	168	–	–	–
8	896	728	–	–	–
12			–	–	–
$L=6$					
0					
4				652	772
8	516	2 030	346	46 484	33 520
12	57 688			1 132 844	711 980
16	201 388	397 360	16 368	13 341 932	6 509 104
20	988 840			29 715 620	13 111 216
24	186 556	241 372$^{1)}$	^{m} 2 736	349 348	58 240$^{1)}$

Table 8. The number of registers distribution depending on nonlinearity and maximum stability for M-NLFSR (if $7 \le L \le 9$ $\deg(f)=2$)

N_f	$sut(f)$, if $m=$		
	0	**1**	**2**
	$L=7$		
0	0	0	0
32	40	716	494
48	7 624	24 862	3 596
56	26 324[1)]	0	0
	$L=8$		
0	0	0	0
64	148	1 578	2 226
96	65 078	380 856	192 572
112	1 620 992	1 737 690	0
	$L=9$		
0	0	0	0
128	200	4398	6 608
192	498 196	4 872 526	4 953 980
224	67 714 544	203 967 024	19 364 756
240	216 743 896	0	0

Table 9. The number of registers distribution depending on nonlinearity and maximum stability for M-NLFSR (if $7 \le L \le 9$ $\deg(f)=2$)

N_f	$sut(f)$, if $m=$			
	3	**4**	**5**	**6**
	$L=7$			
0	0	0	0	–
32	378	[m] 4	–	–
48	0	–	–	–
56	–	–	–	–
	$L=8$			
0	0	0	0	0
64	2 342	188	[m] 42	–
96	14 270	0	–	–
112	0	–	–	–
	$L=9$			
0	0	0	0	0
128	12 198	2 550	848	[m] 10
192	1 079 370	18 642	0	–
224	0	0	–	–
240	0	–	–	–

As it can be seen from the results above, M-NLFSR simultaneously achieve the maximum possible stability and maximum nonlinearity [13-19]. Moreover, all m-optimal functions are also m-saturated (in Tables 6-9 they are marked with «[m]»). In addition, many M-NLFSR functions that are not m-saturated by definition, achieve the highest possible result for the $N_{f\max}(L,m)$ seen above (in the tables 6–9 they are marked with «[1)]»).

Some of the obtained nonlinear recurrent relations of functions that are simultaneously m-optimal and m-saturated and that correspond with M-NLFSR [20-29].

For 2nd order M-NLFSR sized $L=5$ (with nonlinearity N_f = 8 and maximum stability $sut(f)$ = 2, the number of monomials is 6:

$$f = x_2 + x_3 + x_4 + x_5 + x_2 \cdot x_3 + x_1 \cdot x_3$$
$$f = x_1 + x_3 + x_4 + x_5 + x_1 \cdot x_4 + x_1 \cdot x_2$$
$$f = x_1 + x_2 + x_4 + x_5 + x_1 \cdot x_4 + x_3 \cdot x_4$$
$$f = x_1 + x_2 + x_4 + x_5 + x_1 \cdot x_4 + x_1 \cdot x_3$$
$$f = x_1 + x_2 + x_3 + x_5 + x_1 \cdot x_4 + x_1 \cdot x_3$$
$$f = x_1 + x_3 + x_4 + x_5 + x_1 \cdot x_4 + x_2 \cdot x_4$$

For 3rd order M-NLFSR sized $L=6$ (with nonlinearity N_f = 24 and maximum stability $sut(f)$ = 2, 70 functions with 10 monomials, 346 with 12 monomials, 1124 - 14 monomials, 924 - 16 monomials, 252 - 18 monomials, 20 - 20 monomials:

$$f = x_4 + x_5 + x_6 + x_1 \cdot x_2 + x_1 \cdot x_3 + x_2 \cdot x_3 +$$
$$+ x_3 \cdot x_4 + x_1 \cdot x_2 \cdot x_3 + x_1 \cdot x_3 \cdot x_4 + x_1 \cdot x_3 \cdot x_5$$
$$f = x_3 + x_4 + x_5 + x_6 + x_1 \cdot x_2 + x_1 \cdot x_4 + x_2 \cdot x_5 +$$
$$+ x_1 \cdot x_2 \cdot x_3 + x_1 \cdot x_2 \cdot x_4 + x_1 \cdot x_2 \cdot x_5$$

For 2nd order M-NLFSR sized $L=9$ (with nonlinearity N_f = 128 and maximum stability $sut(f)$ = 6, the number of monomials is 10:

$$f = x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_9 + x_2 \cdot x_5 + x_2 \cdot x_8$$
$$f = x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_1 \cdot x_7 + x_4 \cdot x_7$$
$$f = x_1 + x_2 + x_3 + x_4 + x_5 + x_7 + x_8 + x_9 + x_4 \cdot x_6 + x_4 \cdot x_8$$
$$f = x_1 + x_2 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_1 \cdot x_5 + x_3 \cdot x_5$$
$$f = x_1 + x_2 + x_3 + x_4 + x_6 + x_7 + x_8 + x_9 + x_3 \cdot x_5 + x_3 \cdot x_6$$
$$f = x_1 + x_2 + x_3 + x_5 + x_6 + x_7 + x_8 + x_9 + x_3 \cdot x_6 + x_4 \cdot x_6$$
$$f = x_1 + x_2 + x_3 + x_4 + x_6 + x_7 + x_8 + x_9 + x_1 \cdot x_6 + x_5 \cdot x_6$$
$$f = x_1 + x_2 + x_3 + x_5 + x_6 + x_7 + x_8 + x_9 + x_3 \cdot x_4 + x_3 \cdot x_8$$
$$f = x_1 + x_2 + x_3 + x_4 + x_6 + x_7 + x_8 + x_9 + x_2 \cdot x_7 + x_5 \cdot x_7$$
$$f = x_1 + x_2 + x_3 + x_5 + x_6 + x_7 + x_8 + x_9 + x_2 \cdot x_4 + x_2 \cdot x_7$$

By analyzing the results it can be seen that symmetric M-NLFSR have the same $sut(f)$ and N_f. All studied M-NLFSR with $\deg(f) \ge 2$ have $N_f \ge 2^{L-\deg(f)}$.

3. CONCLUSION

This work allows us to obtain and study complete set of M-NLFSR $2 \le L \le 6$, and also $7 \le L \le 9$ the ANF-forming algebraic degree of which is no higher than $\deg(f) \le 2$.

Functions corresponding to M-NLFSR are balanced and have no prohibitions.

Their correlation immunity and nonlinearity is tested and determined. The distribution of the number of M-NLFSR for different values of correlation immunity, nonlinearity, algebraic degree and number of monomials in ANF is given.

It is shown that M-NLFSR achieve the value of the correlation immunity that corresponds to m-optimal functions for all studied L. However, there are a large number of functions that have no correlation immunity. In addition, functions can be m-optimal and m-saturated at the same time.

A number of m-optimal and simultaneously m-saturated functions corresponding to M-NLFSR are given, which also possess the minimum number of ANF monomials, which allows us to minimize costs (temporary and hardware) for generating PRS (for given sizes) on their basis.

Prospective direction of a further research is the argumentation of practical recommendations concerning the implementation of the introduced method and the ways of its use in different mechanisms of an information security of telecommunications networks and systems [30-37].

This research might be useful to us while improving various methods of information security, as well as to other practical applications [38-43].

4. REFERENCES

[1] D. Tang, W.G. Zhang, C. Carlet, X.H. Tang, “Construction of balanced Boolean functions with high nonlinearity and good autocorrelation properties,” *Des. Codes Crypt.*, vol. 67, issue 1, pp. 77-91, 2013.

[2] C. Carlet, “Boolean functions for cryptography and error correcting codes,” *Ch.8 of the Monograph “Boolean Methods and Models in Mathematics, Computer Science, and Engineering”*, Cambridge Univ. Press, 2010. pp. 257–397.

[3] A. A. Kuznetsov, A. V. Potii, N. A. Poluyanenko, I. V. Stelnik, “Nonlinear functions of complication for symmetric stream ciphers,” *Telecommunications and Radio Engineering*, vol. 78, issue 9, pp. 743-458, 2019. DOI: 10.1615/TelecomRadEng.v78.i9.10

[4] A. A. Kuznetsov, A. V. Potii, N. A. Poluyanenko, S. G. Vdovenko, “Combining and filtering functions based on the nonlinear feedback shift registers,” *Telecommunications and Radio Engineering*, vol. 78, issue 10, pp. 853-868. 2019. DOI: 10.1615/TelecomRadEng.v78.i10.20

[5] A. Kuznetsov, O. Potii, N. Poluyanenko, S. Ihnatenko, I. Stelnyk, D. Mialkovsky, “Opportunities to minimize hardware and software costs for implementing Boolean functions in stream ciphers,” *International Journal of Computing*, vol. 18, issue 4, pp. 443-452, 2019. http://computingonline.net/computing/article/view/1614.

[6] J. Sawada, A. Williams, D. Wong, “A surprisingly simple de Bruijn sequence construction,” *Discrete Math.*, vol. 339, pp. 127–131, 2016.

[7] D. Knuth, *The Art of Computer Programming*. Vol. II. Seminumerical Algorithms. USA, *Commonwealth of Massachusetts: Addison-Wesley*, 1969, 634 p.

[8] S. Mesnager, *Bent Functions: Fundamentals and Results*, New York, NY, USA, Springer-Verlag, 2015, 544 p.

[9] S.V. Smyshlyaev, “On the cryptographic weaknesses of some classes of transformations of binary sequences,” *Applied Discrete Mathematics*, vol. 1, pp. 5–15, 2010. (in Russian)

[10] C. Carlet, “Open problems on binary bent functions,” *Lecture Notes in Computer Science, Springer*, pp. 203-241, 2014.

[11] N. Tokareva, *Bent Functions, Results and Applications to Cryptography*, Academic Press, San Diego, CA, 2015, 220 p.

[12] S. Mesnager, “On semi-bent functions and related plateaued functions over the Galois field F2n,” *Proceedings “Open Problems in Mathematics and Computational Science”*, *Lecture Notes in Computer Science*, Springer, pp. 243–273, 2014.

[13] Yu.V. Tarannikov, “On the correlation-immune and stable Boolean functions,” *Mathematical Issues of Cybernetics, Fizmatlit*, vol. 11, pp. 91–148, 2002. (in Russian)

[14] Y. Izbenko, V. Kovtun and A. Kuznetsov, "The design of boolean functions by modified hill climbing method,” *Proceedings of the 2009 Sixth International Conference on Information Technology: New Generations*, Las Vegas, NV, 2009, pp. 356-361.

[15] J. Seberry, X.-M. Zhang and Y.Zheng. “Nonlinearity and propagation characteristics of balanced Boolean functions,” *Information and Computation*, vol. 119, no. 1, pp. 1-13, 1995.

[16] Y. Zheng and X. M. Zhang, “Improved upper bound on the nonlinearity of high order correlation immune functions,” *Selected Areas*

in Cryptography-SAC 2000, *Lecture Notes in Computer Science*, Springer Verlag, vol. 2012, pp. 264–274, 2000.

[17] S. Ronjom, C. Cid, "Nonlinear equivalence of stream ciphers," *Proceedings of the 17th International Workshop on Fast Software Encryption, FSE'2010*, Seoul, Korea, *Lecture Notes in Computer Science*, Vol. 6147, Springer-Verlag, 2010, pp. 40-54

[18] M. Soriano, "Stream ciphers based on NLFSR," *Proceedings of the SBT/IEEE International Telecommunications Symposium ITS'98*, Sao Paulo, Brazil, 1998, vol. 2, pp. 528-533.

[19] J. Szmidt, "Nonlinear feedback shift registers and Zech's logarithms," *Proceedings of the 2019 International Conference on Military Communications and Information Systems (ICMCIS)*, Budva, Montenegro, 2019, pp. 1-4. DOI: 10.1109/ICMCIS.2019.8842713

[20] N. Krishna, V. Murugappan, R. Harish, M. Midhun and E. Prabhu, "Design of a novel reversible NLFSR," *Proceedings of the 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Udupi, 2017, pp. 2279-2283.

[21] O. Kuznetsov, O. Potii, A. Perepelitsyn, D. Ivanenko, N. Poluyanenko, "Lightweight stream ciphers for green IT engineering," *in: Kharchenko V., Kondratenko Y., Kacprzyk J. (eds) Green IT Engineering: Social, Business and Industrial Applications. Studies in Systems, Decision and Control*, vol. 171, Springer, Cham, 2019, pp. 113-137.

[22] S. B. Sadkhan and D. M. Reza, "Investigation of the best structure for the nonlinear combining function," *Proceedings of the 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*, Baghdad, 2017, pp. 180-185.

[23] N. Maeda and A. Tsuneda, "Markov binary sequences generated by post-processing based on feedback shift registers," *Proceedings of the 2019 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, Korea, 2019, pp. 147-149. DOI: 10.1109/ICTC46691.2019.8939599

[24] L. Zhiqiang, "The transformation from the Galois NLFSR to the Fibonacci configuration," *Proceedings of the 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies*, Xi'an, 2013, pp. 335-339.

[25] B. M. Gammel, R. Gottfert and O. Kniffler, "An NLFSR-based stream cipher," *Proceedings of the 2006 IEEE International Symposium on Circuits and Systems*, Island of Kos, 2006, pp. 4 pp.-2920.

[26] A. A. Zadeh and H. M. Heys, "Simple power analysis applied to nonlinear feedback shift registers," *IET Information Security*, vol. 8, no. 3, pp. 188-198, May 2014.

[27] Y. Watanabe, Y. Todo and M. Morii, "New conditional differential cryptanalysis for NLFSR-based stream ciphers and application to grain v1," *Proceedings of the 2016 11th Asia Joint Conference on Information Security (AsiaJCIS)*, Fukuoka, 2016, pp. 115-123.

[28] X. Guo and X. Na, "A research of the Port-Hopping telecommunication techniques based on non-linear feedback shift register (NLFSR)," *Proceedings of the 2011 IEEE International Conference on Automation and Logistics (ICAL)*, Chongqing, 2011, pp. 336-338.

[29] F. Gao, Y. Yang and G. Tan, "Some results on word-oriented nonlinear feedback shift registers," *Proceedings of the 2011 International Conference on Electronics and Optoelectronics*, Dalian, 2011, pp. V4-357-V4-359.

[30] T. Rachwalik, J. Szmidt, R. Wicik and J. Zabłocki, "Generation of nonlinear feedback shift registers with special-purpose hardware," *Proceedings of the 2012 Military Communications and Information Systems Conference (MCC)*, Gdansk, 2012, pp. 1-4.

[31] S. Bondarenko, L. Bodenchuk, O. Krynytska and I. Gayvoronska, "Modelling instruments in risk management," *International Journal of Civil Engineering and Technology*, vol. 10, issue 1, pp. 1561-1568, 2019.

[32] K. Fukuda and A. Tsuneda, "Key-sensitivity improvement of block cipher systems based on nonlinear feedback shift registers," *Proceedings of the 2012 IEEE Asia Pacific Conference on Circuits and Systems*, Kaohsiung, 2012, pp. 100-103. DOI: 10.1109/APCCAS.2012. 6418981

[33] A. Falahati, H. Azizi and R. M. Edwards, "RFID light weight server-less search protocol based on NLFSRs," *Proceedings of the 2016 8th International Symposium on Telecommunications (IST)*, Tehran, 2016, pp. 741-745.

[34] A. Tsuneda, D. Yoshioka and T. Hadate, "Design of spreading sequences with negative auto-correlations realizable by nonlinear feedback shift registers," *Proceedings of the Eighth IEEE International Symposium on Spread Spectrum Techniques and Applications - Programme and Book of Abstract*, Sydney, NSW, Australia, 2004, pp. 330-334. DOI: 10.1109/ISSSTA.2004.1371716

[35] J. Zhong, J. Lu, T. Huang, J. Cao, "Synchronization of mas-tercslave Boolean

networks with impulsive effects: Necessary and sufficient criteria," *Neurocomputing*, vol. 143, no. 143, pp. 269-274, 2014.

[36] J. Zhong and D. Lin, "On minimum period of nonlinear feedback shift registers in grain-like structure," *IEEE Transactions on Information Theory*, vol. 64, no. 9, pp. 6429-6442, Sept. 2018. DOI: 10.1109/TIT.2018.2849392.

[37] K. Runovski, & H. Schmeisser, "On the convergence of fourier means and interpolation means," *Journal of Computational Analysis and Applications*, vol. 6, issue 3, pp. 211-227, 2004.

[38] J. Zhang, T. Tian, W. Qi and Q. Zheng, "A new method for finding affine sub-families of NFSR sequences," *IEEE Transactions on Information Theory*, vol. 65, no. 2, pp. 1249-1257, Feb. 2019. DOI: 10.1109/TIT.2018.2858769

[39] X. Han, Z. Chen, Z. Liu, Q. Zhang, "Calculation of siphons and minimal siphons in Petri nets based on semi-tensor product of matrices," *IEEE Transactions on Systems Man & Cybernetics Systems*, vol. 47, issue 3, pp. 531-536, 2015.

[40] R. Chornei, V. M. Hans Daduna, & P. Knopov, "Controlled markov fields with finite state space on graphs," *Stochastic Models*, vol. 21, issue 4, 847-874, 2005. DOI: 10.1080/ 15326340500294520.

[41] D. W. Zhao, H. P. Peng, L. X. Li, S. L. Hui, Y. X. Yang, "Novel way to research nonlinear feedback shift register," *Science China Information Sciences*, vol. 57, no. 9, pp. 1-14, 2014.

[42] B. P. Tkach, & L. B. Urmancheva, "Numerical-analytic method for finding solutions of systems with distributed parameters and integral condition," *Nonlinear Oscillations*, vol. 12, no. 1, pp. 113-122, 2009. DOI: 10.1007/s11072-009-0064-6.

[43] Y. Yang, X. Zeng and Y. Xu, "Periods on the cascade connection of an LFSR and an NFSR," *Chinese Journal of Electronics*, vol. 28, no. 2, pp. 301-308, 2019. DOI: 10.1049/cje.2019.01. 018.

Alexandr A. Kuznetsov, *Doctor of Sciences (Engineering), Full Professor, Professor of the Department security information systems and technologies of the V. N. Karazin Kharkiv National University. Areas of scientific interests: cryptography and authentication, steganography cybersecurity.*

Oleksandr V. Potii*, Doctor of Sciences (Engineering), Full Professor, Professor of the Department security information systems and technologies of the V. N. Karazin Kharkiv National University. Areas of scientific interests: cryptography and authentication, cybersecurity.*

Nikolay O. Poluyanenko*, Candidate of Technical Sciences (Engineering), Researcher of the Department security information systems and technologies of the V. N. Karazin Kharkiv National University. Areas of scientific interests: cryptography and authentication, cybersecurity.*
Email: nlfsr01@gmail.com

Oleksii A. Smirnov, *Doctor of Sciences (Engineering), Full Professor. Head of Cyber-security & Software Academic Department Central Ukrainian National Technical University, Ukraine. Areas of scientific interests: applied cryptography and coding, security information systems and technologies.*

Igor V. Stelnyk, *Deputy Director of the Department of Information Protection Admini-stration of the State Service of Special Communication and Information Protection of Ukraine. Areas of scientific interests: information and cybersecurity.*

Danylo V. Mialkovsky, *Deputy Director of the Department of Information Protection Admini-stration of the State Service of Special Communication and Information Protection of Ukraine. Areas of scientific interests: information and cybersecurity.*